AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1-32. (Canceled)

33. (Currently amended) A method of generating an Authorized Domain (AD), comprising:

selecting a domain identifier uniquely identifying the Authorized Domain;

directly binding at least one user to the domain identifier; and

obtaining a number of devices and a number of users that are authorized to access a content item of said Authorized Domain, wherein the obtaining step comprises:

binding at least one device to at least one user, such that the at least one device is directly linked to the at least one user and is indirectly linked to the domain identifier through the at least one user, by

obtaining or generating a Device Owner List comprising a unique identifier for a user and a unique identifier for each device belonging to the user, thereby defining that the at least one device is directly bound to the user, or

obtaining or generating a Device Owner List for each device to be bound, the Device Owner List comprising a unique identifier for a user and a unique identifier for a device belonging to the user, thereby defining that the device is directly bound to the user.

34. (Previously presented) The method according to claim 33, wherein each device may be bound to only a single user, or each device may be bound to several users, where one user is indicated as a primary user for that particular device.

35. (Previously presented) The method according to claim 34, further comprising importing, on a given device, at least one content item into the Authorized Domain given by the domain identifier by automatically binding, by default, the at least one imported content item to the single user that the given device is bound to or to the user indicated as primary user for the given device, or binding the at least one imported content item to another user using additional information, when non-default binding is to be used.

36. (Previously presented) The method according to claim 33, further comprising providing an Authorized Domain size limitation, where the limitation relates to a maximum number of users.

37. (Previously presented) The method according to claim 33, further comprising using at least one of:

a user identification device as a personal Authorized Domain manager;

a personal mobile device as a personal Authorized Domain manager;

a mobile phone as a personal Authorized Domain manager; and

a PDA (personal digital assistant) as a personal Authorized Domain manager.

38. (Previously presented) The method according to claim 33, wherein the binding of at least one user to the domain identifier comprises obtaining or generating a Domain Users List comprising the domain identifier and a unique identifier for a user thereby defining that the user is bound to the Authorized Domain.

39. (Previously presented) The method according to claim 33, wherein the binding of at least one content item to the Authorized Domain comprises binding a content item to a User Right, where said User Right is bound to a user bound to the Authorized Domain.

40. (Previously presented) The method according to claim 39, wherein the User Right comprises rights data representing which rights exists in relation to the at least one content item bound to the User Right.

41. (Previously presented) The method according to claim 33, further comprising:

controlling access, by a given device being operated by a given user, to a given content item comprising checking whether a user, the given content item is linked to, and a user, the given device is linked to, belongs to the same Authorized Domain, and

allowing access for the given user and/or other users via the given device to the content item if so, and/or

checking if the given content item is linked to a user belonging to the same Authorized Domain as the given user, and

allowing access for the given user via the given device and/or other devices to the content item if so.

42. (Previously presented) The method according to claim 33, further comprising:

controlling access, by a given device being operated by a given user, to a given content item being bound to the Authorized Domain and having a unique content identifier, wherein controlling access comprises:

checking if the user bound to the given device is bound to the same Authorized Domain as the user bound to the content item, by

checking if the Domain User List of the Authorized Domain comprises:

a first user identifier, wherein a Device Owner List comprises an identifier of the given device and the first user identifier, and

a second user identifier, linked to the given content item; and

allowing access to the given content item by the given device operated by any user and/or checking if the Domain User List of the Authorized Domain, that the content item is bound to, comprises a user identifier of the given user thereby checking if the given user is bound to the same Authorized Domain as the content item, and allowing access to the given content item by any device including the given device operated by the given user.

43. (Previously presented) The method according to claim 41, wherein the controlling of access of a given content item comprises checking that the User Right for the given content item specifies that the given user has the right to access the given content item and only allowing access to the given content item in the affirmative.

44. (Previously presented) The method according to claim 33, wherein every content item is encrypted and that a content right is bound to each content item and to a User Right, and that the content right of a given content item comprises a decryption key for decrypting the given content item.

45. (Previously presented) The method according to claim 38, wherein the Domain Users List is implemented as or included in a Domain Users Certificate, and/or the Device Owner List is implemented as or included in a Device Owner Certificate, and/or the User Right is implemented as or included in a User Right Certificate.

46. (Previously presented) The method according to claim 33, further comprising binding at least one content item to at least one user.

47. (Currently amended) A system for generating an Authorized Domain, comprising:

means for obtaining a domain identifier uniquely identifying the Authorized Domain;

means for directly binding at least one user to the domain identifier; and

means for obtaining a number of devices and a number of users that are authorized to access a content item of said Authorized Domain, wherein the means for obtaining comprises:

means for binding at least one device to at least one user, such that the at least one device is directly linked to the at least one user and is indirectly linked to the domain identifier through the at least one user, by

obtaining or generating a Device Owner List comprising a unique identifier for a user and a unique identifier for each device belonging to the user thereby defining that the at least one device is directly bound to the user, or

obtaining or generating a Device Owner List for each device to be bound, the Device Owner List comprising a unique identifier for a user and a unique identifier for a device belonging to the user thereby defining that the device is directly bound to the user.

48. (Previously presented) The system according to claim 47, wherein each device may be bound to only a single user, or each device may be bound to several users, where one user is indicated as a primary user for that particular device.

49. (Previously presented) The system according to claim 48, further comprising means for importing, on a given device, at least one content item into the Authorized Domain given by the domain identifier by automatically binding, by default, the at least one imported content item to the single user that the given device is bound to or to the user indicated as primary user for the given device, or binding the at least one imported content item to another user using additional information, when non-default binding is to be used.

50. (Previously presented) The system according to claims 47, further comprising means for providing an Authorized Domain size limitation, where the limitation relates to a maximum number of users.

51. (Previously presented) The system according to claim 47, further comprising at least one of:

means for using a user identification device as a personal Authorized Domain manager;

means for using a personal mobile device as a personal Authorized Domain manager;

means for using a mobile phone as a personal Authorized Domain manager; and

means for using a PDA (personal digital assistant) as a personal Authorized Domain manager.

52. (Previously presented) The system according to claim 47, wherein the means for binding at least one user to the domain identifier is adapted to obtain or generate a Domain Users List comprising the domain identifier and a unique identifier for a user, thereby defining that the user is bound to the Authorized Domain.

53. (Previously presented) The system according to claim 47, wherein the means for binding at least one content item to the Authorized Domain is adapted to bind a content item to a User Right, where said User Right is bound to a user bound to the Authorized Domain.

54. (Previously presented) The system according to claim 53, wherein the User Right comprises rights data representing which rights exists in relation to the at least one content item bound to the User Right.

55. (Previously presented) The system according to claim 47, further comprising means for controlling access, by a given device being operated by a given user, to a given content item, is adapted to check whether a user, the given content item is linked to, and a user, the given device is linked to, belongs to the same Authorized Domain, and allowing access for the given user and/or other users via the given device to the content item if so, and/or check if the given content item is linked to a user belonging to the same Authorized Domain as the given user, and allowing access for the given user via the given device and/or other devices to the content item if so.

56. (Previously presented) The system according to claim 52, further comprising means for controlling access, by a given device being operated by a given user, to a given content item being bound to the Authorized Domain and having a unique content identifier, where the means for controlling access is configured to:

check if the user bound to the given device is bound to the same Authorized Doman as the user bound to the content item, by

checking if the Domain User List of the Authorized Domain comprises:

a first user identifier, wherein a Device Owner List comprises an identifier of the given device and the first user identifier, and

a second user identifier, linked to the given content item; and

allow access to the given content item by the given device operated by any user and/or check if the Domain User List of the Authorized Domain, that the content item is bound to, comprises a user identifier of the given user thereby checking if the given user is bound to the same Authorized Domain as the content item, and allow access to the given content item by any device including the given device operated by the given user.

57. (Previously presented) The system according to claim 55, wherein the means for controlling access of a given content item is further adapted to check that the User Right for the given content item specifies that the given user has the right to access the given content item and only allow access to the given content item in the affirmative.

58. (Previously presented) The system according to claim 47, wherein every content item is encrypted and that a content right is bound to each content item and to a User Right, and that the content right of a given content item comprises a decryption key for decrypting the given content item.

59. (Previously presented) The system according to claim 51, wherein the Domain Users List is implemented as or included in a Domain Users Certificate, and/or the Device Owner List is implemented as or included in a Device Owner Certificate, and/or the User Right is implemented as or included in a User Right Certificate.

60. (Currently amended) A computer readable storage medium having stored thereon instructions for causing one or more processing units to execute actions comprising:

selecting a domain identifier uniquely identifying the Authorized Domain directly binding at least one user to the domain identifier; and

obtaining a number of devices and a number of users that are authorized to access a content item of said Authorized Domain, wherein the obtaining step comprises:

binding at least one device to at least one user, such that the at least one device is directly linked to the at least one user and is indirectly linked to the domain identifier through the at least one user, by

obtaining or generating a Device Owner List comprising a unique identifier for a user and a unique identifier for each device belonging to the user, thereby defining that the at least one device is directly bound to the user, or

obtaining or generating a Device Owner List for each device to be bound, the Device Owner List comprising a unique identifier for a user and a unique identifier for a device belonging to the user, thereby defining that the device is directly bound to the user.